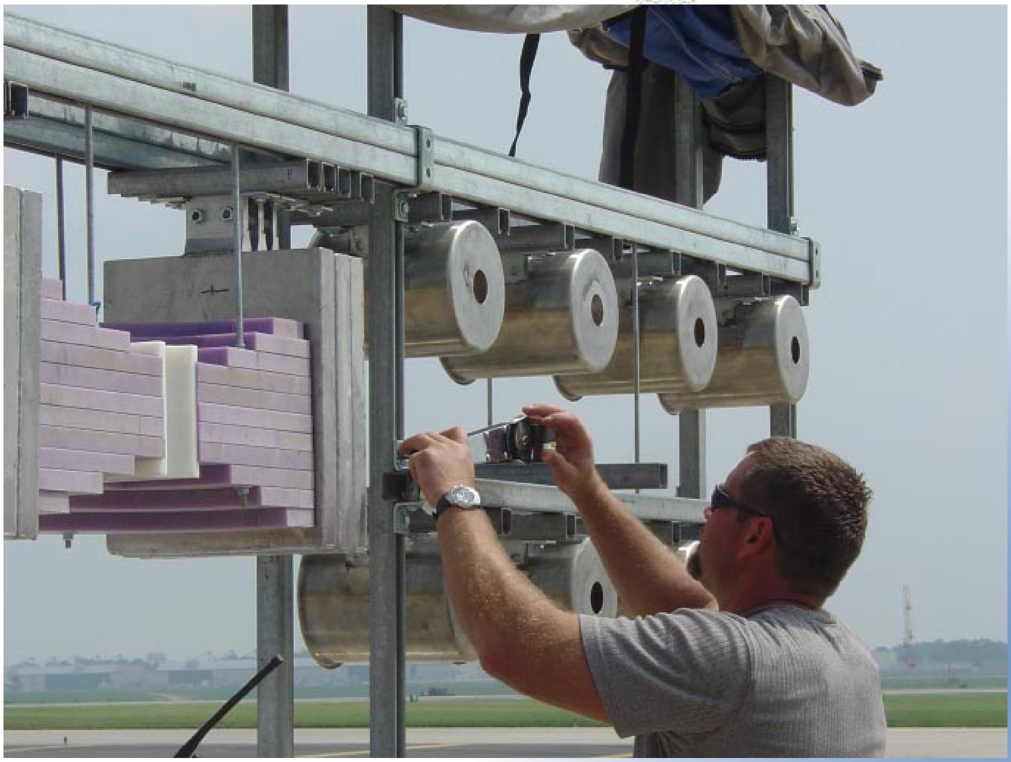
NEED TO KNOW

a national security newsletter

Volume 5, Number 1 November 2004



Jeff Klinger, INEEL Explosives Detection System program manager, performs a quality inspection of the assembled IEDS at Andrews Air Force Base. The INEEL patent-pending detection system uses neutron activation technology in a portal-type configuration, employing a technique called pulsed thermal neutron analysis.

INEEL Tackles Global Threat of Terrorist Bombings

Hardly a day goes by without some news account of the devastation wrought by an explosion. Russia, Iraq, Spain or the United States – no country is immune to the fear and danger spread by terrorist bombings.

Scientists and engineers at the INEEL have been working on a practical solution to reduce threats from improvised explosives. In July, they proved it could work.

Under the looming presence of Air Force One, military and federal eyewitnesses lined up to observe as trucks with potentially lethal cargo entered the scorpionlike pincers of INEEL’s explosive detection system. The nonintrusive, noncontact inspection technique successfully identified – within 300 seconds – the contents of each truck as carrying explosives or not.

System Design

INEEL’s Explosive Detection System (IEDS) is designed to interrogate cargo trucks. Use of IEDS could eliminate the type of terrorist attack that occurred in Oklahoma City, where a truck laden with over 4,000 pounds of explosives destroyed the Alfred P. Murrah Federal Building.

“No single technology eliminates all threats,” said Jeff Klinger, IEDS program manager. “For example, this technology doesn’t address suicide bombers. But if we stop one bombing, save one life, then I think we are successful.”

The system won’t replace explosives-sniffing dogs either, the foundation of most detection programs. But dogs and handlers – with costs rivaling even the most comprehensive technologies – can’t work 24/7/365. Machines can. The IEDS system, like others the government is evaluating, would supplement dogs and other processes currently in place.

Using the INEEL system, trucks or automobiles entering a government building parking garage, military base or embassy grounds – or passing through a checkpoint – would be required to stop within the system’s inspection zone. After the driver exits the vehicle, the IEDS process would begin.

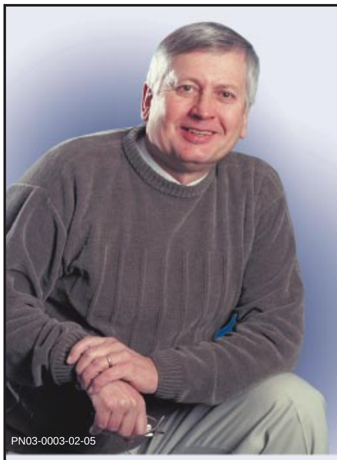
The INEEL patent-pending detection system uses neutron activation technology in a portal-

See **EXPLOSIVES**, *page 2*

IDAHO NATIONAL ENGINEERING AND ENVIRONMENTAL LABORATORY

INEEL

Home of Science
and Engineering Solutions



State of the Division

Laurin Dodd,
Associate Laboratory Director, National Security

This edition of *Need to Know* is the final one to be issued as an INEEL publication. As we go to press, DOE has announced its selection of Battelle Energy Alliance as the contractor team that will be honored – and challenged – to create and manage the new Idaho National Laboratory. This is an exciting time for all of us. The future is bright for both the new laboratory and the National Security Division.

For all involved, being in on the ground floor in the creation of a new national laboratory will be both challenging and rewarding.

The Idaho National Laboratory, officially slated to come into being the first of February, combines the INEEL – minus the waste management operations – with Argonne National Laboratory-West. The new laboratory is expected to start with a staff of about 3,000 and an annual budget in excess of $400 million. It will be a multiprogram laboratory with a focus on nuclear energy and national security. Within national security, the focus will be critical infrastructure protection and nonproliferation.

Those of us within the National Security Division take considerable pride in 'creating' the national security focus. Over the last five years, the national security R&D business has quadrupled. Combined with armor manufacturing at SMC and the Navy-sponsored ATR mission, a broadly defined national security business will represent roughly half of the business as the new laboratory emerges.

Staff and management within the National Security Division, with guidance from our External Review Board, have created the critical infrastructure mission over the last several years. This has resulted in the formation of numerous test beds and a 'national' critical infrastructure test range. Today, we are working with numerous clients from across government and industry in addressing problems that are important to our nation's security.

I congratulate my national security colleagues for what they have accomplished during the last several years. And I thank our clients for giving us the opportunity to work with them. I can assure them that the transition to the INL will be a positive event for them in both the near term and the longer term.

The 'engineering can-do' attitude that exists at the INEEL today, combined with laboratory policies and procedures unconstrained by the cleanup mission, will assure a bright future for staff engaged in national security programs with the new Idaho National Laboratory.

EXPLOSIVES

(continued from page 1)

type configuration. Employing a technique called pulsed thermal neutron analysis, the system puts out high-energy neutrons to cause nuclear excitation of materials within the vehicle. Sodium iodine detectors identify elements within the targeted cargo that indicate the presence of explosives. The whole process takes about five minutes and leaves no lasting radiation effects on the inspected truck or cargo.

"Our job was to get working hardware on the ground," said Klinger. "Our customer believes that while science is good for scientists, products are good for people. So we conducted proof-of-principal tests using existing technologies to develop our path forward."

Klinger worked with an integrated team consisting of physicists Ed Reber, Keith Jewell and Ed Seabury, mechanical engineers Phil West and Brion Bennett, radiological engineer Andy Edwards, software designers Ken Rohde and Kurt Derr, systems engineer Mindy Kirkpatrick, statistician Larry Blackwood and mechanical designer Rich Watson. The team tested accelerators, radioactive sources and neutron generators to select the neutron generating source. While all produced satisfactory results, accelerators and other active sources were eliminated as choices. Active sources, such as californium used in INEEL's successful portable isotopic neutron spectroscopy, require special handling, and the accelerators generated much more energy than the system needed. Neutron generators with their on/off switch are inherently safer and are scaled at the right energy level.

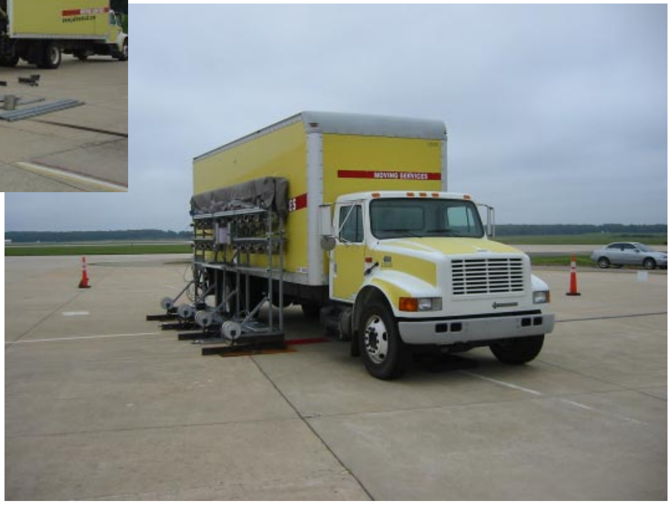
"Why use a sledgehammer when a ball-peen hammer will do," said Klinger.

They selected the sodium iodine detectors over the more sensitive germanium detectors for several reasons. Germanium detectors require cooling by liquid nitrogen for operation and are extremely expensive. Customer direction called for the best – but also the

Explosives like these are easy to conceal in medium-sized panel trucks. Without even touching the truck, the IEDS can detect the presence of explosives in under five minutes.

most cost-effective solutions. The IEDS team concluded that the sodium iodine detectors would perform more consistently under a wider range of environmental conditions, and their cost would be more conducive to the numbers needed for mass production. IEDS design calls for an array of 32 detectors, 16 on each side.

The IEDS team arrives at Andrews Air Force Base and organizes the system's components prior to assembly (left). With assembly complete, the explosive detection system is nearly ready to show what it can do (below).



The INEEL system is quick, inexpensive and reliable, due in part to its simple, yet robust design that incorporates few moving parts that can break down. The team's design incorporated much commercially available hardware, further reducing costs and enabling future "plug-and-play" improvements as industry advances.

The laboratory's expertise and many of its patents will come from the innovative integrated engineering and algorithms that correctly interpret the raw data and make the determination that explosives are – or are not – present.

The team also designed the system to monitor the health of its individual components, so an operator could quickly pinpoint potential problems and make adjustments. The graphical user interfaces – what the operator sees on the computer screen – are easy to understand and eliminate potential for ambiguous interpretation. The IEDS – like other INEEL technologies fielded at home and abroad – is designed for reliable operation by a technician or soldier and requires minimal training.

Next Phase

Now that the demonstration has proven the viability of the system, the IEDS team is tasked to design a system that industry can build. Initial negotiations for manufacture have already begun.

"The threat is not diminishing," said Klinger. "In fact, if anything, it is growing. So we have to get something on the ground fast, while at the same time work to improve the speed, sensitivity and robustness of the system."

The INEEL is pursuing a cooperative research agreement with an American manufacturer of neutron generators. Right now, the generators in the IEDS experimental system come from France and were originally designed for scientific and medical applications. Klinger wants a tough box that will handle desert-to-tropical environments and the manhandling of the real world versus the white-glove treatment in a laboratory or hospital.

Even as the team is designing the Phase III system with its manufacturing specifications, Klinger is contemplating future applications, including land mine detection, mass transit baggage inspection and robotic cargo container checks.

"An important role of national laboratories today is to mitigate threats against our citizens and our soldiers," said INEEL Laboratory Director Paul Kearns. "The INEEL has an outstanding history of developing sensors to detect chemical weapons and nuclear materials. Now we're building on that legacy of excellence to stop would-be bombers."

Jeff Klinger
klinjb@inel.gov

As Air Force One thunders by, the assembled INEEL Explosive Detection System sits enshrouded within its cloth covers. Unlike explosive-sniffing dogs, technologies like IEDS can work 24/7/365.

Team members James Hanneman, Hope Forsmann, and Lynda Brighton (left to right) are working with colleagues Nancy Johnson, Allen Anderson and John Svoboda to develop a "smart antenna" system.

Antennas go to the Head of the Class at INEEL

Contributed by Regina Nuzzo

Wireless hotspots are cropping up nearly everywhere these days. Coffee houses and college campuses, large office buildings and living rooms – even entire towns are being rigged with access points that blanket an area with wireless Internet access.

But covering large swaths of land with network access isn't always efficient or even desirable. Instead of using one large umbrella over an entire area, designers may prefer an access point that can hand out the equivalent of personal raincoats, giving network coverage that follows individual users – while leaving hackers unprotected and out in the storm.

For that kind of flexible coverage, antennas that send out network signals from access points need to be brainier than their average cousins. INEEL engineer Lynda Brighton and her colleagues Hope Forsmann, Allen Anderson, Nancy Johnson, John Svoboda and James Hanneman are working on ways to combine several antenna elements into one sophisticated "smart antenna" system. This will help wireless local area networks (WLAN) reach farther, juggle more users, navigate tricky environments, avoid electronic interference, and protect against rogue users.

Ultimately, the INEEL engineers hope to give WLAN users a more cost-efficient bang for their buck. "For wireless networks today," Brighton says, "it's crucial that solutions are affordable." WLAN access points will need to work in increasingly demanding environments, she says. And right now, designers are bumping up against some simple geometry problems. Simple problems, perhaps, but ones with intricate solutions.

Traditional WLAN Antennas: One Umbrella

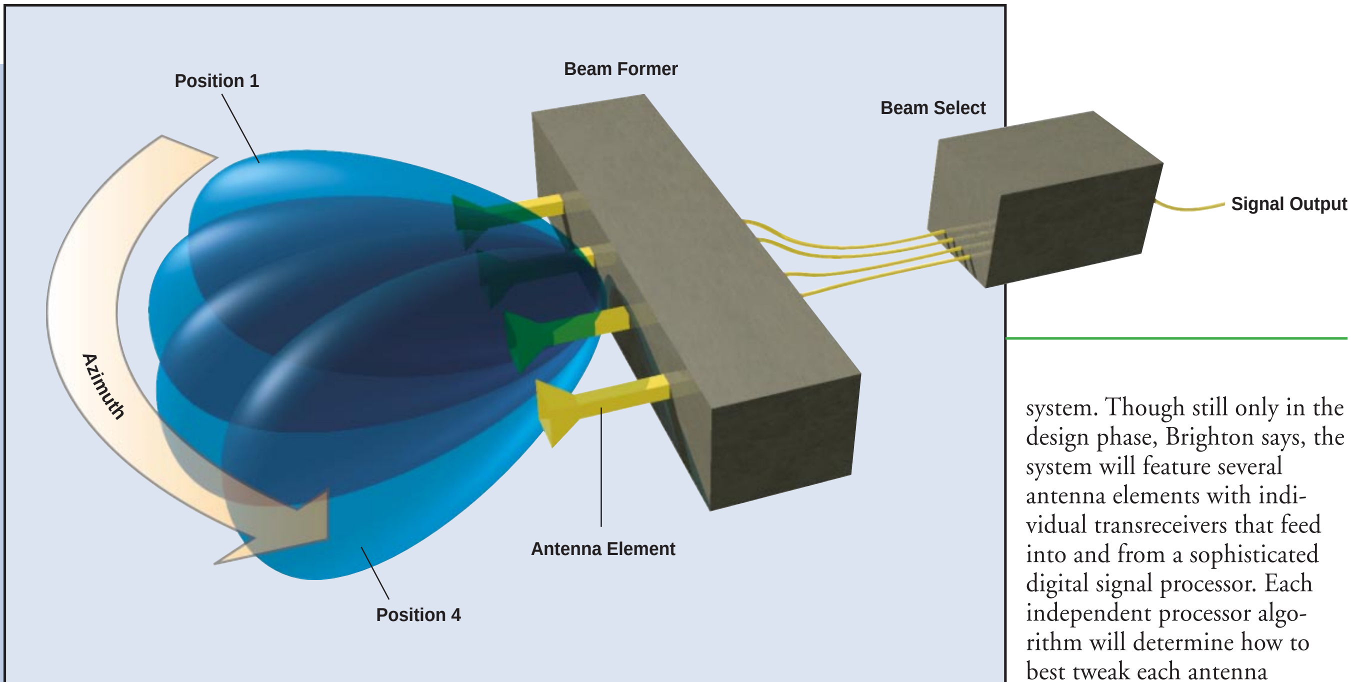
Wireless Internet networks work on the same principles as cordless phones. A roaming laptop and a fixed access point – plugged into the Internet through a cable modem or DSL – communicate with each other through embedded antennas and exchange information over certain radio frequencies.

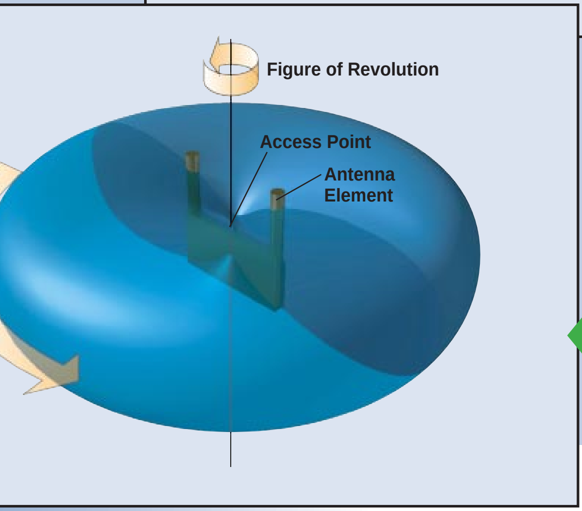
Typical access points use omni-directional antennas, which transmit and receive signals all around it, Brighton says. "Its coverage is shaped like a doughnut. It's equal in all directions along the horizon and then gradually decreases as you look up or down, with a small hole in the middle where the antenna itself is." In ideal situations, omni-directional antennas can handle the job well. But in the real world, umbrella coverage has its limitations.

One problem is that the traditional doughnut shape can be a waste of energy, Brighton says. A large umbrella will cover every user within a fixed area and none beyond. So wireless networks can't selectively exclude some users near the antenna or extend coverage to others slightly farther away. And since WLANs use radio frequencies shared by other electronics – such as cordless phones, microwave ovens, and other WLANs – an access point may run into interference from other equipment, Brighton says.

Also, standard antennas work best when there's a clear line of sight between the access point and users, Brighton says. But objects such as walls or furniture typically clutter WLAN environments and bounce signals around. The antenna indiscriminately picks up all signals within range, both direct and reflected. Called the multipath problem by antenna engineers, this can mean fluctuating service for connected users.

Finally, traditional access points face limited bandwidth because a typical access point uses only one frequency channel. A single laptop can exchange information with the access point at the





Smart Antenna: A digital signal processor and a beamformer algorithm are used to create simultaneous beams from antenna elements and point them in a variety of directions.

Traditional Antenna: The beam from a single antenna element extends omni-directionally in a doughnut shape.

fastest possible rate. Add an extra user with the same load, though, and “it’s like the data pipe is now split in half,” Brighton explains. Each user can work at only half the maximum speed. As the number of users climbs, bandwidth drops proportionally, and even high-speed connections can easily slow to a crawl.

Smart Improvements in Smaller Packages

But a so-called smart antenna system can circumvent many of these problems. It features a choreographed array of antenna elements that focuses its energy on a smaller, grape-shaped area instead of the traditional wide doughnut. Smart systems take advantage of a central processor to monitor users, control the beams, and customize the coverage area. And the smarter the antenna, the more customized the shape.

Processors in simple smart systems can switch among several fixed antenna beam directions to find the clearest signal from a laptop. Slightly more advanced smart antennas can steer beams across an arc to hone in on a user. And best yet are adaptive systems, which continually mix information from a large array of antenna elements to give a highly customized, amoeba-shaped coverage area – extending range in some directions, blocking out narrow slivers of area in others, all while sorting through shifting multipath signals.

Mixed Signals, More Adaptability

The newest WLAN antenna technology has been made possible only recently with advances in other fields – namely, cheaper and smaller processors. Brighton’s group tested two new, just-on-the-market smart antenna systems and a traditional omni-directional one, comparing a variety of performance measures.

They’re putting these lessons to use by designing an even smarter, adaptive antenna system. Though still only in the design phase, Brighton says, the system will feature several antenna elements with individual transreceivers that feed into and from a sophisticated digital signal processor. Each independent processor algorithm will determine how to best tweak each antenna element to optimize energy in one direction while minimizing energy in all others. This, she explains, will minimize effects of interference and multipath while also increasing range and blocking unwanted users. And since independent digital beams are formed, each user will get virtually no drop in bandwidth, no matter how many users are connected – though limited, of course, by processor and Internet connectivity capabilities. What’s more, she says, a technique called Doppler shift removal will let the system track and adapt to moving users in real time.

The trick, Brighton says, is designing the adaptive antenna system to be affordable, which means using existing transreceiver and digital signal processor technologies. “The hardware is an integral part of the system, but we don’t want to mess with that part. Whether we can build something with off-the-shelf components – that is a real challenge.”

Lynda Brighton
brigll@inel.gov

INEEL Protects U.S. Infrastructures from Digital Terrorism

Contributed by Ethan Huffman

Cyber security researchers Kevin Lackey (left) and Jared Verba discuss the software coding of a computer virus in this photo taken at the INEEL's Control System Security and Test Center.

On July 13, 2004, Muhammad Naeem Noor Khan, a 25-year-old computer engineer, was captured by U.S. officials in Islamabad, Pakistan, leading to a chain reaction of arrests in Britain and an elevated terror warning for the U.S. financial district. Evidence collected during his arrest, including a laptop loaded with images, drawings and layouts of potential U.S. targets, provided credible proof of what U.S. officials have long suspected. Al Qaeda, and other terrorist networks, are quickly gaining the necessary skills and abilities to potentially launch a cyber attack on the United States.

In a 2003 Dartmouth College report entitled *Examining the Cyber Capabilities of Islamic Terrorist Groups,* evidence suggests that al Qaeda operatives have spent time on sites that offer software and programming instructions for control systems, the digital switches that run power, water, transportation and communications grids.

The potential of a cyber attack has been well documented in the United States, too. In a 2003 Government Accountability Report (04-321), the FBI confirmed that terrorists, transnational criminals and intelligence services are becoming aware of and using information exploitation tools such as computer viruses, Trojan horses, worms, logic bombs and eavesdropping sniffers that can destroy, intercept, degrade the integrity of or deny access to data.

This information, though alarming, has been a high priority for all government agencies, including the Department of Energy, since 9/11. At the INEEL, targeted research, tool development and training is being conducted to protect the nation's critical infrastructures from a cyber attack before one occurs.

The Control System Security and Test Center, located at the Information Operations Research Center in Idaho Falls, Idaho, is aimed at protecting the nation's critical infrastructures from cyber attacks.

Vulnerabilities

Most control systems, such as Supervisory Control and Data Acquisition, or SCADA systems – typically used in the energy industry – were designed and built for efficiency and reliability, not security. During the mid-1990s as corporations were beginning to provide e-commerce services online, many control systems were also networked to the Internet so activities could be monitored from corporate headquarters or at remote stations, limiting the physical number and cost of technical employees.

The result of linking control systems to the Internet left them wide open for a cyber attack. However, emphasis was not placed on securing these systems beyond a standard firewall because traditional hackers had been more interested in exploiting large-scale, iconic targets such as government agencies and Fortune 500 companies. That changed after 9/11, when the federal government realized the motivation for terrorist attacks against the United States was to destroy economic stability and endanger public safety.

Today, evidence clearly supports the intent of terrorist groups to gain and utilize cyber attacks as a means of creating chaos. With concerns such as these, the U.S. Departments of Energy and Homeland Security selected the

INEEL to lead the nation in securing critical infrastructures.

Work at the INEEL

This summer, the INEEL received $10 million from the Department of Homeland Security's National Cyber Security Division to begin a control systems security and testing program. The INEEL officially launched the Control System Security and Test Center (CSSTC) in its newly renovated state-of-the-art Information Operations Research Center in August. The CSSTC program creates a centralized location where utility companies, equipment manufacturers and government agencies can work together to find solutions and reduce vulnerabilities in control systems. The intent is to reduce the probability of a cyber attack on the nation's critical infrastructures.

The CSSTC program also functions in a supporting role to the U.S. Computer Emergency Readiness Team, or CERT. If a major cyber attack were launched against control systems, the U.S. CERT may call upon a staff of experts at the INEEL to provide technical assistance and help get the affected systems back online.

The program operates a multi-functional cyber security test bed capable of running mock attacks and calculated scenarios similar to traditional attacks used by hackers and U.S. adversaries. This type of research allows customers to visualize the effects of a control system cyber attack without the real-life consequences.

Also housed within the Information Operations Research Center and working in concert with the CSSTC is the National SCADA Test Bed. Funded by the Department of Energy's Office of Energy Assurance and run in collaboration with Sandia National Laboratories, the National SCADA Test Bed consists of functioning control systems from national and international manufacturers.

The CSSTC program leverages other research capabilities from the numerous test beds located within the INEEL complex, including a wireless telecommunication system and a full-sized electrical power distribution structure, and at other DOE labs nationwide. These test beds will provide data and tools for strengthening customer systems.

The INEEL has established working relationships with more than 30 utility companies and equipment manufacturers.

Julio Rodriguez
Ju2@inel.gov

Leader of the Pack

Some people say tragedy can be turned to triumph. For Kansas State University student and INEEL summer intern Renee Ecklund, the tragedy occurred one fall morning while she sat in a university speech class three years ago this September.

"All I remember hearing was airplanes and buildings," said Ecklund, remembering the first few moments after a student had told the class about the 9/11 terrorist attacks. "I managed to make it to the student union building and saw everyone huddled around the television screens. I watched as the second tower collapsed."

The images, news reports and uncertainty haunted the electrical engineering student much as they did everyone else. But that's where this story takes an ironic turn. Shortly after the events of that day, the United States created the Department of Homeland Security, and with it, a scholarship budget for college students interested in pursuing careers in homeland security. For Ecklund, that meant an opportunity to apply for a scholarship that paid part of her education, complete a government internship, and pursue a career that is not only interesting, but also challenging and meaningful.

"It [the scholarship] has really been a life-changing event for me," said Ecklund. "It's strange to think that because of the attacks, I'm sitting here today."

Last summer, Ecklund was one of six national security interns who spent 10 weeks at the INEEL working on a variety of projects. For her part, Ecklund developed and created a computer-aided visual model and map of one of the INEEL's electrical substations. This substation, known as SPERT (originally supporting the Special Power Excursion Reactor Test), is part of a chain of power transmission lines that feed power to INEEL buildings and electrical components. The model she developed is used to educate lab customers and visitors on power distribution and infrastructure protection at the INEEL, the state of Idaho and even the western half of the United States.

Department of Homeland Security intern, Renee Ecklund, builds maps and graphical representations of the INEEL electrical power distribution system.

"We wanted to give her something to work on that would help her in school and educate her," said Sam Bader, Ecklund's project mentor. "She was top gun, an excellent performer and very focused on her work."

Ideally, Ecklund hopes to use her education to do advanced research in alternative power sources such as wind power. For now, she will spend a second year in the DHS scholarship program at Kansas State and possibly return to the INEEL next summer.

Perhaps better than anyone else, Ecklund understands the irony of her story. With the memories of 9/11 still present, it's strange to think that a day of tragedy could yield a positive direction for a group of young students. As we pass the three-year anniversary of Sept.11, it appears that young students, like Ecklund, are rapidly becoming homeland security leaders for their generation.

The Art of Elicitation

Contributed by Chris Crandall
Counterintelligence Officer

A casual conversation with a co-worker, business colleague, client or friend is not only a process of communication, but also a technique used to collect and share information. From the Counterintelligence perspective, this subtle method of extracting desired information is referred to as **elicitation.** We all do it and for various reasons. So why should we be concerned?

In the hands of a highly skilled intelligence collector, an elicitation session can garner a wealth of information without ever raising an eyebrow from the person being interviewed. Elicitation is never adversarial in tone or character and is usually performed without direct questioning. The whole purpose of elicitation is to obtain information from someone who has it, without that person becoming sensitive to the purpose of the information collector.

Intelligence collectors will often know something about the personality type of their subject that helps the elicitation process progress. For example, they may know if the person is an introvert or extrovert; intuitive or sensing; thinking or feeling; or perhaps judging or perceiving. The demographics of where people live and generally what they do for a living can provide valuable insight into the make-up of a potential target.

Successful elicitation is a learned technique; it is the art of inducing another person to talk, guiding a conversation by concealing the true purpose, asking the right questions in the right way at the right time, and making the conversation interesting to a target. The following tips will help you recognize if someone is attempting to elicit information from you.

- A provocative statement is generally made to induce a question in response.
- Quid Pro Quo – you share something and the collector shares something.
- Word repetition or active listening provides an opportunity to expand on what has already been said.
- Competitive positioning allows the collector to disagree with you so that you can set him/her straight.
- Sharing of common points of interest.
- Naiveté allows you to be an instructor and demonstrate your knowledge or expertise about a topic.

If you believe that you are being drawn into a conversation that is making you feel uncomfortable, consider the following countermeasures:

- You are under no obligation to tell anyone anything they are not authorized to hear.
- Ignore the question and change the topic.
- Deflect their question with one of your own.
- Give a nondescript answer.
- "I don't know," is a perfectly acceptable response.
- Avoid the individual.
- You can always suggest that you would need to clear such discussions with your Counterintelligence office.

Most people like talking about themselves, their work, families or hobbies. We like others to believe we are the expert, which makes it tempting to demonstrate our expertise and knowledge. Most importantly, when engaging in any work-related discussions, be sure you have a clear understanding of what you can and cannot talk about. Because elicitation is so subtle and difficult to recognize, it is important to report any suspicious conversations to the INEEL Counterintelligence office. Remember, when traveling or interacting with foreign nationals, exert care and caution.

Don't become a target of elicitation. Even casual, seemingly innocuous conversations can be designed to surreptitiously extract information from you.

NEED TO KNOW *is a publication of the National Security Division of the Idaho National Engineering and Environmental Laboratory. The INEEL is a science-based, applied engineering national laboratory dedicated to supporting the U.S. Department of Energy's missions in environment, energy, science and national security. The INEEL is operated for the DOE by Bechtel BWXT Idaho, LLC. Requests for additional copies, story ideas or questions should be directed to the editor at (208) 526-1058, kzc@inel.gov. This is printed on recycled paper.*

Editor .... Kathy Gatens
Graphic artist .... David Combs
Photographers .. Mike Crane, Chris Morgan, Ron Paarmann
Copy editing ...... Rick Bolton
Research .... Steve Paschke

Visit our national security website at:
www.inel.gov/nationalsecurity